

Data Governance Challenges in Virtualised & Cloud Infrastructures

Visibility through Encryption



Russell Dietz

CVP & Chief Technology Officer (CTO)

Russell.Dietz@safenet-inc.com

@russdietz - twitter

May 2011

AusCERT2011

10th Annual AusCERT
Information Security Conference

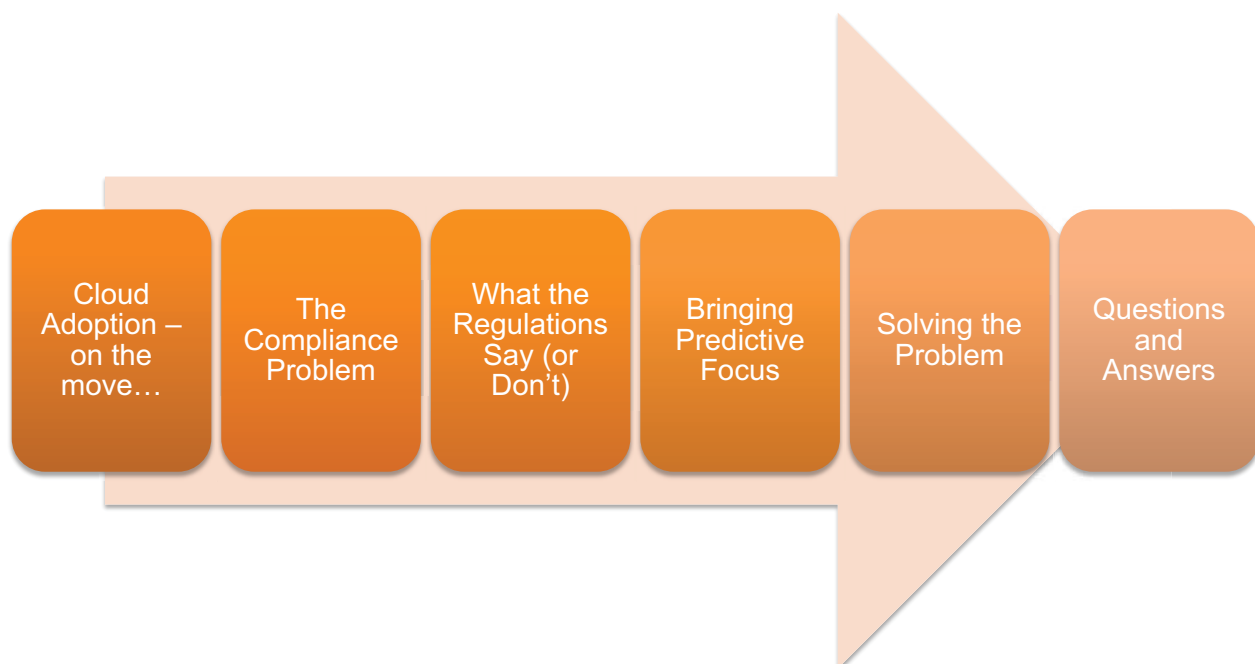
15th - 20th May 2011

OVEREXPOSED



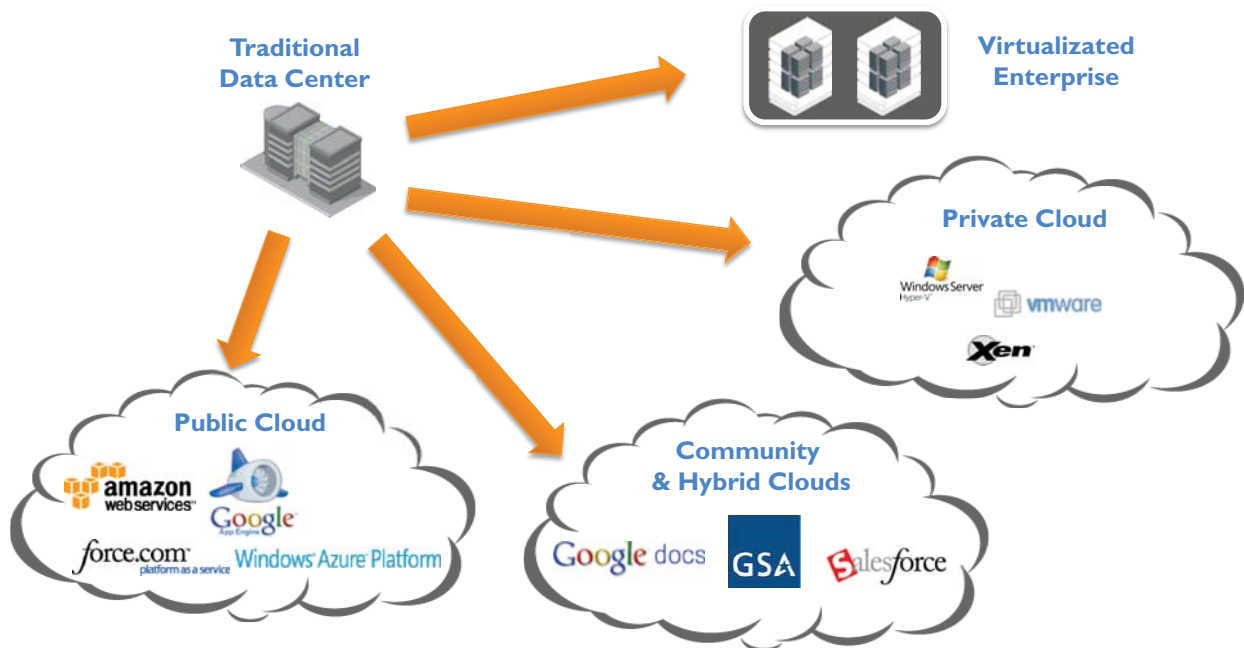
AusCERT

Agenda

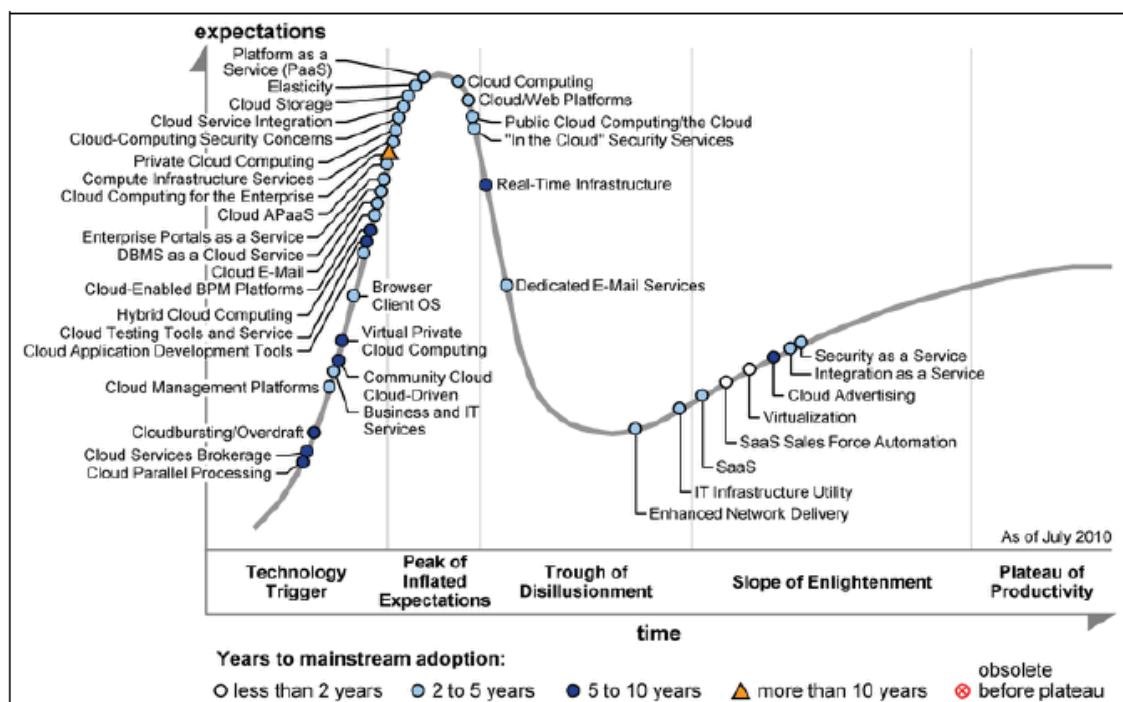


Cloud delivery models – all at once!

Cloud & Virtualization Adoption... on the rise



Global Cloud Adoption – Moving fast...



* Gartner July 2010 – Cloud Hype Cycle



Market Growth in Cloud Computing

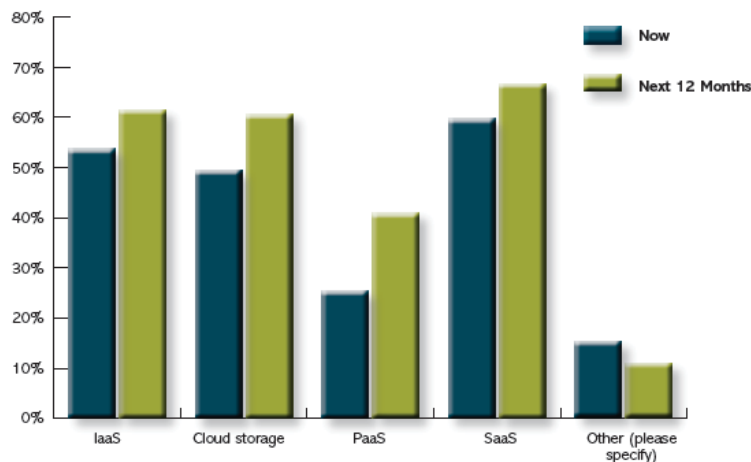
Over 60% of enterprises plan to evaluate or pilot some type of cloud-enabled offerings within the next 18 months. However, enterprises continue to delay cloud adoption due to concerns surrounding data security, privacy and compliance

(Gartner Hype Cycle for Cloud Computing, 2010, David Mitchell Smith, July 27, 2010)

Server revenue in the public cloud category will grow from \$582 million in 2009 to **\$718 million** in 2014; Server revenue for the private cloud market will grow from **\$7.3 billion** to \$11.8 billion

(IDC, May 2010)

FIGURE 4: IN THE CLOUD STACK, WHICH SERVICES DOES/WILL THE COMPANY USE?



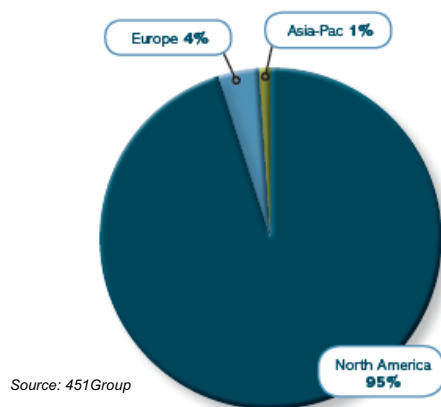
SMB spending on cloud computing will approach **\$100 billion** by 2014

(AMI Partners, August 2010)



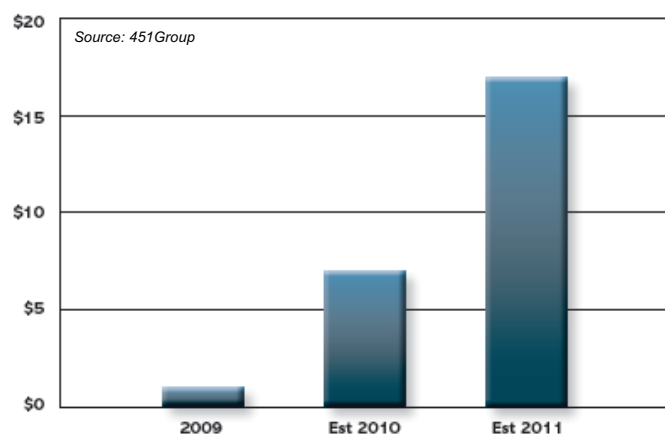
Asia-Pac & Cloud – Early Days...

FIGURE 1: ESTIMATED 2010 REGIONAL REVENUE BREAKDOWN



Source: 451Group

FIGURE 2: CLOUD SERVICE REVENUES IN ASIA-PACIFIC, 2009-2011 (\$M)



Source: 451Group



Australia's Cloud Governance & Guidance



Australian Government
Department of Finance and Deregulation

Cloud Computing Strategy - April 2011

Layer	Example	Data Centre with Adv. Virtualization	Private ⁹ Cloud	Hybrid cloud	Community Cloud (Incl. G-Cloud)	Public Cloud
Information and Services layers						
Citizen-facing services	Citizen-driven (joined-up) service delivery (lines of business)	Now-5 years				3-5 years
Business Processes	Consolidated or shared business processes, for example, Financial, HR, Budgeting, Procurement, content management, case management	Now-5 years				3-5 years
Applications	Custom applications/Packaged applications/external services	Now-5 years				3-5 years
Citizen information	Concerns individual citizens, covered by privacy and data protection (security)	1-2 years		3-5 years		6-10 years
Public Information	Open government data / mashups Collaborative tools, e.g. blogs, wikis, data.gov.au					Now
Technology layer						
Channels (online)	Government websites and portals Web2.0 technologies (e.g. gmail) Discovery tools, for example Google Search			Now		Now
Technology (infrastructure)	IT and telecommunication infrastructure – utility model	Now				
Technology (process / storage capability)	Process and analyse large datasets Use as a storage platform	Now				



Australian Government
Department of Defence

Defense Signals Directorate

Cloud Computing Security - April 2011

- a. availability of data and business functionality;
- b. protecting data from unauthorised access; and,
- c. handling security incidents.



7

Trust is THE issue!

IT Security is stopping projects. Compliance/Audit has tons of questions. Cloud growth IS being limited. All the birds are dead.



IT Security Group: The cloud isn't secure. I don't trust Providers. I don't know how to secure that thing!

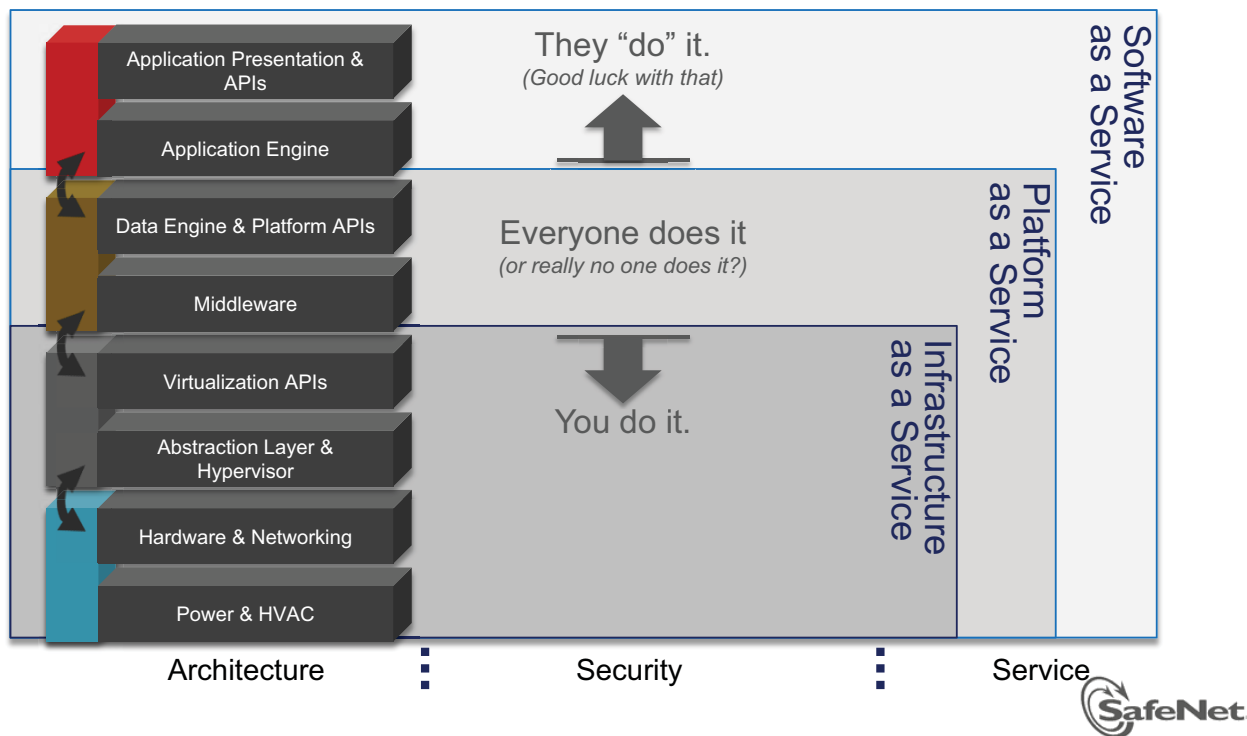
Compliance Audit Group: Show me your security. Prove compliance in Clouds. Convince me!



8

Cloud Architectures

Varying Levels of Abstraction and Data Ownership



Cloud Security Challenges

	IaaS	PaaS	SaaS
User ID and Access: Secure Authentication, Authorization, Logging			X
★ Data Co-Mingling: Multi-tenant data mixing, leakage, ownership			X
Application Vulnerabilities: Exposed vulnerabilities and response			X
Insecure Application APIs: Application injection and tampering			X
★ Data Leakage: Isolating data		X	X
Platform Vulnerabilities: Exposed vulnerabilities and response		X	X
Insecure Platform APIs: Instance manipulation and tampering		X	X
★ Data Location/ Residency: Geographic regulatory requirements		X	X
Hypervisor Vulnerabilities: Virtualization vulnerabilities	X	X	X
Data Retention: Secure deletion of data	X	X	X
★ Application & Service Hijacking: Malicious application usage	X	X	X
★ Privileged Users: Super-user abuse	X	X	X
Service Outage: Availability	X	X	X
Malicious Insider: Reconnaissance, manipulation, tampering	X	X	X
Logging & Forensics: Incident response, liability limitation	X	X	X
Perimeter/ Network Security: Secure isolation and access	X	X	X
Physical Security: Direct tampering and theft	X	X	X

Fundamental Trust & Liability Issues

- Data exposure in multi-tenant environments
- Separation of duties from cloud provider insiders
- Transfer of liability by cloud providers to data owners

Fundamental New Cloud Risks

- New hypervisor technologies and architectures
- Redefine trust and attestation in cloud environments

Regulatory Uncertainty in the Cloud

- Regulations likely to require strong controls in the cloud

Trust & Hypervisors Challenge Us to Do Better

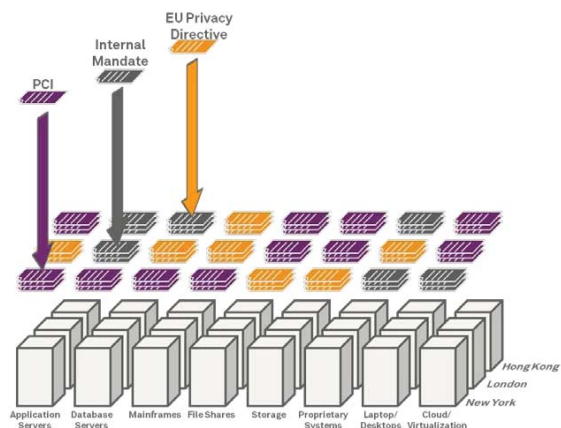
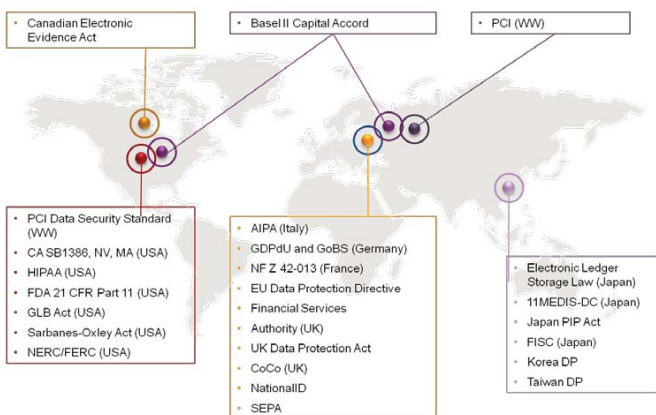
And encryption hits trust and isolation head-on



Regulations Will Impact Cloud

- Many regulations
- That often overlap

Worldwide Compliance Requirements



Let's take a quick look at PCI

- Number of times “cloud” is mentioned in PCI DSS 2.0 = 0

2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) <i>Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.</i>	2.2.1.a For a sample of system components, verify that only one primary function is implemented per server. 2.2.1.b If virtualization technologies are used, verify that only one primary function is implemented per virtual system component or device.
--	--

- Virtualization just made it into 2.0
- But we already know, Service Providers subject to PCI



The Truth- You Are On Your Own for Now

- Bad News: Confusing Regulatory Landscape
 - Shared responsibility model- but demarcation is gray
 - SAS 70 inadequate for common use in evaluating cloud providers
 - Formal transfer of liability highly likely written into your cloud contract
 - You will have to have a detailed architecture and API conversation to assess your responsibility
- Good News: Everyone Trying to Solve the Problem
 - XaaS know this, working hard to alleviate
 - Cloud Security Alliance has Mapping Document

So where do we go from here???



- Focus on First Principles
 - Spirit and intent of regulations
 - Thoughtful data handling
- Sprinkled with the “New” Cloud Issues
 - These are where regulations will focus
 - Will be around the new area we discussed before:
 - Trust and Ownership
 - Hypervisors
 - Disclosure and Visibility



15

First Principles and Cloud Challenges

Principle	Trust/Ownership	Hypervisor	Disclosure/Visibility	Issues
Limit use of <sensitive data>			X	Big issue in SaaS, in your control for the most part in IaaS and PaaS
Use secure development practices			X	Issue in SaaS and PaaS
★ Control access to <sensitive data>	X	X	X	Issues in all cases. Issues of user identification, authorization rights, privileged cloud user
Encrypt <sensitive data> in transit	X		X	Most likely already addressed, but customer to cloud, intracloud communication can be an issue
★ Optional <sensitive data> encrypt at rest	X		X	Huge issue in data sitting in the cloud, across all platforms.
★ Keep <sensitive data> confidential	X	X	X	Main issue is guaranteeing the “trust” in data when you don’t “trust” the cloud.
★ Keep the integrity of <sensitive data>	X	X	X	Main issue is guaranteeing the “trust” in data when you don’t “trust” the cloud.
★ Enforce separation of duties of <sensitive data> access and administration	X	X	X	Fundamental issue of cloud employee and cloud administrator access. Extends to both physical and logical security. Invokes separation of duties issues around all controls.
★ Report and audit your controls for			X	Can you prove it to your auditor.

et.

16

Emergence of Encryption as a Unifying Cloud Security Control

Strong encryption with key management is one of the core mechanisms that Cloud Computing systems should use to protect data. While encryption itself doesn't necessarily prevent data loss, as harbor provisions in laws and regulations treat lost encrypted data as not lost at all. The encryption provides resource protection while key management enables access to protected resources.



- Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing"

Companies are looking to protect data in the cloud through encryption keys and robust key management. This enables companies to secure data from breaches as well as prevent the cloud provider from accessing the information if they decide to end their relationship with the cloud provider.



- Frost and Sullivan, Michael Suby

Encryption is one of the best ways to secure corporate data in the cloud, but it has to be encryption that the company controls.



- Forrester Research, Jonathan Penn

Encryption is a fundamental technology for realizing cloud security

- Isolate data in multi-tenant environments
- Recognized universally by analysts and experts and underlying control for cloud data
- Sets a high-water mark for demonstrating regulatory compliance adherence for data

■ Moves from Data Center tactic to Cloud strategic solution

- Physical controls, underlying trust in processes, and isolation mitigated some use of encryption
- Mitigating trust factors that don't exist in the cloud.



How Encryption Solves Main Pain Points

Principle	Trust/Ownership	Hypervisor	Disclosure/Visibility	Issues
Limit use of <sensitive data>			X	Big issue in SaaS, in your control for the most part in IaaS and PaaS
Use secure development practices			X	Issue in SaaS and PaaS
Control access to <sensitive data>	Encryption enables authentication and authorization layer.			
Encrypt <sensitive data> in transit			X	Most likely already addressed, but customer to cloud, intracloud communication can be an issue
Optional <sensitive data> encrypt at rest	Encryption directly addresses many regulator requirements. Shows high standard of care.			
Keep <sensitive data> confidential	Encryption fundamentally isolates your data from other tenants in a share cloud environment, shields from unauthorized data breach.			
Keep the integrity of <sensitive data>	Encryption inherently provides for integrity controls.			
Enforce separation of duties of <sensitive data> access and administration	Encryption can add additional authentication and authorization layer for users and administrators. Customer owned encryption definitively shows separation from cloud.			
Report and audit your controls for	Encryption Key ownership is tangible proof to data ownership. Encrypt/Decrypt actions become easy log and audit proofs.			

Encryption- Additional Upside



“Lawful Order” to Cloud Provider for Data

Issue: Cloud provider may turn over your data when another member of the cloud is under criminal investigation. Your data is now viewable to law enforcement.

Resolution: Encrypted data unviewable by law enforcement. Law enforcement would have to work through legal channels, under which you have guaranteed rights, to get you to turn over decryption keys.



Destruction of Cloud Data

Issue: Is data in the cloud ever destroyed? Are you sure?

Resolution: Encryption makes data unusable in the cloud. “Key shredding” virtually makes encrypted cloud data unrecoverable



Physical Location Issues of Cloud Data

Issue: Is cloud data now in new physical locations requiring new regulatory insight, or violates existing regulatory law?

Resolution: Encrypted data can be moved anywhere in the cloud, but controlled decryption with proper key release policy can define what localities may use data.



19

Encryption Your Biggest Tool, Not Perfect

Hypervisor Security

- Data could be exposed when running, even when encrypted.
- Is an issue you need to deal with no matter what
- Combination of vetting cloud provider controls of hypervisor security, deploying specific hypervisor tools (monitoring and integrity tools), and isolating data through encryption

Instance Snapshotting and Storage

- Could store “running” instances, expose keys and cleartext
- An issue to discuss with your cloud provider
- Amazon AWS- has thought about this, and therefore only allows storing of AMIs in down state, thus eliminating problem
- Not all cloud providers are as wise

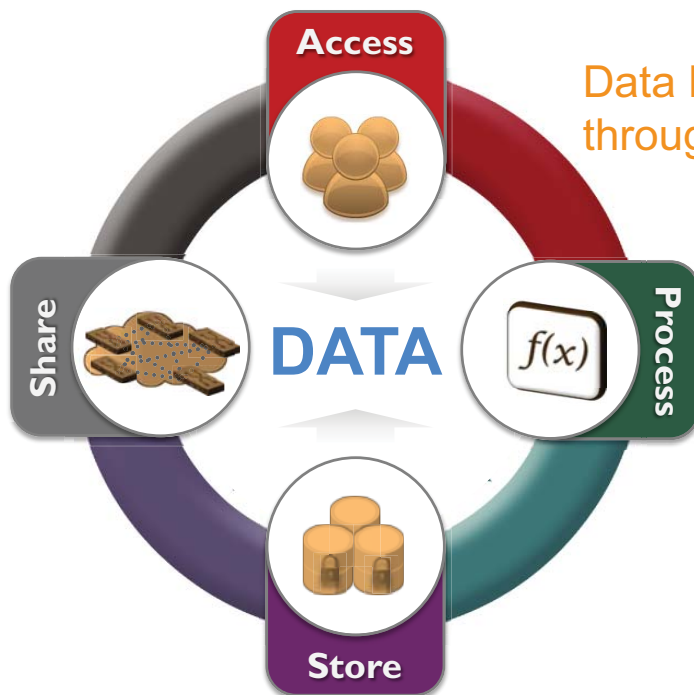
Proper Key Handling

- When you do encryption, is the key properly stored and handled? Many regulations give specific key handling requirements (security, state, rotation, etc.).
- If your cloud provider is doing encryption for you, huge issues in key ownership. If they maintain the keys, you lose almost all separation of duties and visibility controls.
- Key granularity an issue- some cloud providers use a single key for all their customers!!!



20

Protect the Data Where it Lives



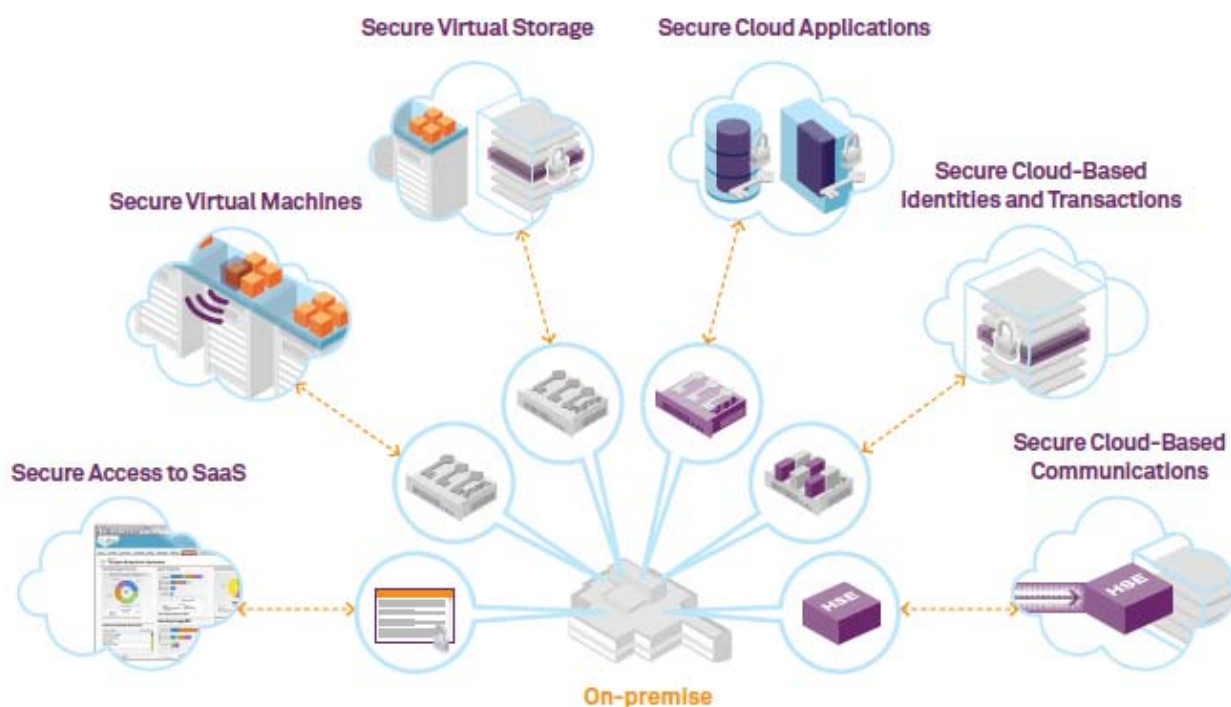
Data Protection should follow it through its lifecycle

- know what users, applications, or instances **Access Data**.
- Secure the **Data Processing** during the creation, analytic, aggregation, and modification of the data.
- Apply consistent data protection policy across any **Data Store**.
- Enforce data privacy controls while **Sharing Data**, with threat protections inherent in that sharing.



SafeNet Trusted Cloud Fabric

Maintaining Trust and Control in Virtualized Environments



Additional Resources

Cloud Security Alliance

- > Excellent
- > Vendor Neutral

SafeNet Website

www.safenet-inc.com/cloudsecurity

- > Videos
- > White Papers
- > Additional Resources



23



Questions?

Visibility through Encryption

Russell Dietz

CVP & Chief Technology Officer (CTO)

Russell.Dietz@safenet-inc.com

@russtdietz - twitter

May 2011

AusCERT2011

10th Annual AusCERT
Information Security Conference

15th - 20th May 2011

OVEREXPOSED

